

NEW APPLICATION FEE TRANSMITTAL

Attorney Docket No. 1614.1085
 Application Number
 Filing Date October 11, 2000

AMOUNT ENCLOSED \$ 970.00

First Named Inventor Syuichi SATAKE



FEE CALCULATION (fees effective 10/01/97)

CLAIMS	(1) FOR	(2) NUMBER FILED	(3) NUMBER EXTRA	(4) RATE	(5) CALCULATIONS
	TOTAL CLAIMS	12 - 20 =	0	X \$ 18.00 =	\$ 0.00
	INDEPENDENT CLAIMS	6 - 3 =	3	X \$ 80.00 =	240.00
	MULTIPLE DEPENDENT CLAIMS (any number; if applicable)			+ \$240.00 =	0.00
	BASIC FILING FEE				710.00
	Total of above Calculations =				\$ 930.00
	Surcharge for late filing fee, Statement or Power of Attorney (\$130.00)				+ 0.00
	Reduction by 50% for filing by small entity (37 CFR 1.9, 1.27 & 1.28).				- 0.00
	TOTAL FILING FEE =				\$ 930.00
	Surcharge for filing non-English language application (\$130.00; 37 CFR 1.52(d))				+ 0.00
	Recordation of Assignment (\$40.00; 37 CFR 1.21(h)(1))				+ 40.00
	TOTAL FEES DUE =				\$ 970.00

METHOD OF PAYMENT

- ☒ Check enclosed as payment.
☐ Charge "TOTAL FEES DUE" to the Deposit Account No., below.
☐ No payment is enclosed and no charges to the Deposit Account are authorized at this time.

GENERAL AUTHORIZATION

- ☒ If the above-noted "AMOUNT ENCLOSED" is not correct, the Commissioner is hereby authorized to credit any overpayment or charge any additional fees necessary to:

Deposit Account No. 19-3935

Deposit Account Name STAAS & HALSEY LLP

- ☒ The Commissioner is also authorized to credit any overpayments or charge any additional fees required under 37 CFR 1.16 (filing fees) or 37 CFR 1.17 (processing fees) during the prosecution of this application, including any related application(s) claiming benefit hereof pursuant to 35 USC § 120 (e.g., continuations/divisionals/CIPs under 37 CFR 1.53(b) and/or continuations/divisionals/CPAs under 37 CFR 1.53(d)) to maintain pendency hereof or of any such related application.

SUBMITTED BY: STAAS & HALSEY LLP

Typed Name	H. J. Staas	Reg. No.	22,010
Signature		Date	October 11, 2000

0968353 10100

SPECIFICATION

TO ALL WHOM IT MAY CONCERN:

BE IT KNOWN THAT I, Syuichi Satake, a citizen of Japan residing at Nei, Japan have invented certain new and useful improvements in

APPARATUS AND METHOD FOR AUTHENTICATING
DIGITAL SIGNATURES AND COMPUTER-READABLE
RECORDING MEDIUM THEREOF

of which the following is a specification : -

TITLE OF THE INVENTION

APPARATUS AND METHOD FOR AUTHENTICATING
DIGITAL SIGNATURES AND COMPUTER-READABLE RECORDING
MEDIUM THEREOF

5

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention generally relates to
apparatuses and methods for authenticating digital
10 signatures and computer-readable recording media
having a program recorded therein for causing a
computer to authenticate a digital signature, and
more particularly to an apparatus and a method for
authenticating a digital signature, and a computer-
15 readable recording medium having a program recorded
therein for causing a computer to authenticate a
digital signature, in which apparatus, method and
medium the digital signature is formed by a random
unintelligible number or character string and a
20 signature mark of a signer can be built into image
information so that the digital signature can be
visually recognized.

2. Description of the Related Art

In a network such as a client/server
25 system shown in Fig.1, a plurality of clients and a
server are connected through the network. In such a
network system, an electronic decision system is
widely known in which a decision transaction is
conducted by utilizing GroupWare.

30 In the electronic decision system, a
digital signature is used. For example, in Fig.1, a
user A of a client A attaches a digital signature to
a document created by the user A and then sends the
document to a user B of a client B through the
35 network. The user B of the client B obtains a public
key for decrypting the digital signature of the user
A of the client A and decrypts the digital signature

0968559 101100

5
10

15

20

25

30

35

SUMMARY OF THE INVENTION

It is a general object of the present invention to provide an apparatus for authenticating a digital signature in which the above-mentioned problems are eliminated.

A more specific object of the present invention is to provide an apparatus and a method for authenticating a digital signature, and a computer-readable recording medium having a program recorded therein for causing a computer to authenticate a digital signature, in which apparatus, method and medium the digital signature is formed by a random unintelligible number or character string and a signature mark of a signer can be built into image information so that the digital signature can be visually recognized.

The above objects of the present invention are achieved by an apparatus for authenticating a digital signature, including: a signature generating part encrypting a digital document by using a private key defined by a signer and digest information for checking whether the digital document has been tampered with, and generating a digital signature; a signature synthesizing part creating image information by synthesizing the digital signature and a predetermined mark; and an image embedding part embedding the image information created by the signature synthesizing part into an indicated position in the digital document.

According to the present invention, the digital signature is created by encrypting the private key for authenticating the signer and the digest key for validating the digital document. Further, the digital signature is built in the image information and then the image information including the digital signature is embedded in the digital

5

10

25

35

tampered with, and generating a digital signature;
(b) creating image information by synthesizing the
digital signature and a predetermined mark; and (c)
embedding the image information created in the step
5 (b) into an indicated position in the digital
document.

According to the present invention, it is
possible to provide the method for authenticating a
digital signature in which method the digital
10 signature, which is generated from a random number or
character string, can be imaged to be visually
recognizable.

The above objects of the present invention
are also achieved by a method for authenticating a
15 digital signature, including the steps of: (a)
extracting the digital signature from image
information embedded into a digital document; (b)
decrypting the digital signature by a public key
opened by a signer and obtaining first digest
20 information for checking whether the digital document
has been tampered with; and (c) determining whether
second digest information regenerated based on the
digital document identically corresponds to the first
digest information obtained by the step (b) and
25 authenticating the digital signature based on a
result of the determination.

According to the present invention, it is
possible to provide the method for authenticating a
digital signature in which method the signer can be
30 authenticated and the digital document can be
validated simultaneously.

Furthermore, the above objects of the
present invention are achieved by a computer-readable
recording medium having a program recorded therein
35 for causing a computer to authenticate a digital
signature, including the codes of: (a) encrypting a
digital document by using a private key defined by a

09685859 101100

signer and digest information for checking whether the digital document has been tampered with, and generating a digital signature; (b) creating image information by synthesizing the digital signature and a predetermined mark; and (c) embedding the image information created in the step (b) into an indicated position in the digital document.

According to the present invention, it can be realized by a computer installing the codes from the computer-readable recording medium that the digital signature, which is generated from a random number or character string, can be imaged to be visually recognize.

The above objects of the present invention are achieved by a computer-readable recording medium having a program recorded therein for causing a computer to authenticate a digital signature, including the codes of: (a) extracting the digital signature from image information embedded into a digital document; (b) decrypting the digital signature by a public key opened by a signer and obtaining first digest information for checking whether the digital document has been tampered with; and (c) determining whether second digest information regenerated based on the digital document identically corresponds to the first digest information obtained by the code (b) and authenticating the digital signature based on a result of the determination.

According to the present invention, it can be realized by a computer installing the codes from the computer-readable recording medium that the signer can be authenticated and the digital document can be validated simultaneously.

BRIEF DESCRIPTION OF THE DRAWINGS

Other objects, features and advantages of the present invention will become more apparent from

05635859 101100

FIG.1 is a diagram illustrating a client/server system;

FIG.3 is a flowchart for explaining a
10 registration process for seal information;

15 FIG.5 is a flowchart for explaining a
process for embedding the seal image into a document;

FIG.7 is a flowchart for explaining processes for authenticating the digital signature;

FIG.9 is a diagram illustrating another authentication result window when the stamped seal image is not authenticated; and

35 DESCRIPTION OF THE PREFERRED EMBODIMENTS

FIG.2 is a block diagram of a hardware configuration of an apparatus for authenticating a

digital signature according to an embodiment of the present invention.

In FIG.2, the apparatus as a computer system includes a CPU (Central Processing Unit) 11, a
5 memory unit 12, an input unit 14, a display unit 15, a storage unit 16, a CD-ROM driver 17 and a communication unit 18, which are mutually connected by a bus B.

The CPU 11 controls the entire computer
10 system in accordance with a program resident in the memory unit 12. In addition, the CPU 11 executes processes for authenticating a digital signature that will be described later. The memory unit 12 includes ROM and RAM. Also, the memory unit 12 temporarily
15 stores programs and various data necessary for or obtained from executions of the processes. In addition, a part of the memory unit 12 is assigned as a working area accessed by CPU 11.

The input unit 14 includes a keyboard and
20 a mouse but is not limited to only these input devices. The input unit 14 is used for a user to register and change information for an authentication process, and to input information into the computer system. The display unit 15 displays results of
25 various processes or data necessary for the user.

The storage unit 16 includes a hard disk and stores various data and programs.

In accordance with instructions from the CPU 11, the CD-ROM driver 17 reads information from
30 the CD-ROM 20 set in the CD-ROM driver 17 and then provides the information to the storage unit 16. For example, various programs according to the present invention are provided by the CD-ROM 20. That is, the programs read from the CD-ROM 20 are installed in
35 the storage unit 16 through the CD-ROM driver 17. It should be noted that a recording medium is not limited to the CD-ROM 20, but another computer-

09685859 101100

Introduction

Introduction

[illegible][illegible]

then clicks "STAMP" on the execution window 61 (step S12). By clicking "STAMP", the CPU 11 in FIG.2 of the client A used by the user A generates an MD (message digest) file (or digest information) ensuring contents of the document created by the user A (sealed document) (step S13). Subsequently, the CPU 11 encrypts the digest information generated in the step S13 (step S14). Accordingly, the digital signature, which is formed by an unintelligible number or character string, is created by encrypting the digest information in accordance with a predetermined method based on the private key defined by the user A.

The CPU 11 searches the storage unit 16 in FIG.2 for seal image data registered by the user A based on the employee number and the seal name indicated by the user A on the execution window 61.

The CPU 11 regenerates the seal image from the seal image obtained from the storage unit 16 (step S15). The digital signature created from the digest information is embedded into the seal image regenerated in the step S15 (step S16). In detail, a process for building the digital signature into the seal image will be described later. The seal image the built-in digital signature is embedded into the area 63 of the document, which was indicated by the user A when the execution window 61 was opened. Then the seal image is displayed as an embedded seal image in an embedded area 67 of the document in FIG.6B and the confirmation window 65 shown in FIG.6B is displayed on the document (step S17). When the user A clicks "OK", it is confirmed that the seal image is to be embedded into the document. The process is then completed.

Accordingly, the digital signature can be embedded with the seal image into the document such as an HTML (Hyper Text Markup Language), an SGML

seal area 83 and obtains the digital signature, that is, the random number or character string (step S43).

The CPU 11 decrypts the digital signature by the public key obtained in the step S42. Since
5 the digital signature was encrypted by digest information and the private key of the user A, the digest information is extracted after the digital signature is decrypted (step S44). Hereinafter, the digest information may be referred to as decrypted
10 digest information.

Furthermore, the CPU 11 regenerates an MD file (regenerated digest information) of the document received from the user A (step S45). Subsequently, the CPU 11 compares the decrypted digest information
15 extracted by decrypting the digital signature in the step S44 with the regenerated digest information regenerated in the step S45 (step S46) and notifies the user B of a comparison result as an authentication result by displaying the
20 authentication result window 85 (step S47). When the regenerated digest information identically corresponds to the decrypted digest information, the authentication result window 85 shown in FIG.8B is displayed at the display unit 15 in FIG.2 so as to
25 notify the user B that the seal image stamped on the document received from the user A is valid. That is, the legal digest information is obtained in the step S44 and then the user A as a writer is authenticated and it is verified that the document received from
30 the user A has not been tampered with. On the other hand, when the regenerated digest information does not identically correspond to the decrypted digest information, another authentication result window 91 shown in FIG.9 is displayed at the display unit 15 so
35 as to notify the user B that the seal image stamped on the document received from the user A is invalid. That is, the user A as a writer is invalid or the

document received from the user A has been tampered with, or both the user A and the document are invalid.

The process for building the digital signature into the seal image will be now described
5 in details with reference to FIGS.10A, 10B and 10C.

Referring to FIG.5, the CPU 11 of the client A at the sender side obtains the private key input by the user A on the execution window 61 shown in FIG.6A (step S12). The CPU 11 generates the
10 digital signature shown in FIG.10A by encrypting the digest information generated in the step S13 by an encryption function. For the sake of convenience, a hex number is used in FIG.10A.

Subsequently, the CPU 11 obtains the seal
15 image generated in the step S15. The seal image is formed by pixel data (bitmap data) and each pixel data is an index number indicating a palette position. In the embedded area 67 of the document that is confirmed on the confirmation window 65 shown in
20 FIG.6B, for example, a background color is white and a seal color (character color) is black. In this case, the pixel data of the seal image obtained is formed by a plurality of index numbers indicating white or black. The CPU 11 replaces the index
25 numbers indicating colors other than the character color (white) with data (hex numbers) of the digital signature from a beginning of the pixel data. For example, when the seal image is created, the character color of the seal image is always defined
30 at a beginning of the palette. Since the index number of black is "00 (hex)", the CPU 11 replaces the index numbers with the data of the digital signature while skipping "00 (hex)" in the data of the digital signature. In a header part (not shown)
35 of the seal image including the pixel data, information indicating data lengths of the seal image and the digital signature is additionally provided.

09685859 101100

The CPU 11 may set color data (for example, RGB data) indicating white to palette positions other than a palette position for black since the palette positions for 256 colors are indicated by the index numbers "00 (hex)" through "FF (hex)". In this case, the CPU 11 sets white color data to palette positions indicated by the index numbers "01 (hex)" through "FF (hex)" other than the palette position for black as the character color indicated by the index number "00 (hex)". Accordingly, as shown in FIG.10C, a palette is created such that the character color is black and background color is white. Thus, the digital signature, which is encrypted and becomes an unintelligible long string, can be built into the seal image so that the user B does not have to be bothered by the unintelligible long string. Also, it is not required to transform the seal image so that the user B can easily distinguish the seal image of the user A by sight.

As described above, the document, which has been embedded therein the seal image having the built-in digital signature is sent to the user B. A process for decrypting the seal image received from the user A will now be described with reference to FIG.10A and FIG.10B.

Referring to FIG.7, in the client B as a receiver, the seal image is extracted by indicating the seal area 83 in FIG.8A on the document received from the user A (the step S41). The pixel data (bitmap data) forming the seal image is shown in FIG.10B. The CPU 11 of the client B obtains the information including the data lengths of the seal image and the digital signature from the header of the seal image. In this case, since the character color is indicated by the index number "00 (hex)", the CPU 11 reads the pixel data from the beginning of the seal image while skipping "00 (hex)" in the pixel

data. Then, the CPU 11 extracts the digital signature shown in FIG.10A (the step S43).

Subsequently, the CPU 11 decrypts the digital signature extracted in the step S43 by using
5 the public key obtained in the step S42 and a function such as a decryption function. Then, the digest information is obtained (the step S44).

In the embodiment, the user B obtains the public key from a server providing the public key
10 list. Alternatively, the client A as a sender may set information including the name and the employee number of the user A in the header of the seal image so that the client B as a receiver can obtain the public key from the server. Thus, it is not required
15 for the user B using the client B to access the server to obtain the public key.

Moreover, in the embodiment, the digital signature is built in the background of the seal image. Alternatively, in FIG.10C, instead of "black"
20 indicated by the index number "00 (hex)", "white" can be applied as the character color and instead of "white" indicated by the index numbers "01 (hex)" through "FF (hex)", "black" can be applied as the background color.

25 According to the present invention, the digital signature is built into an image so as to be imaged. That is, the imaged digital signature, which is generated from a random number or character string, can be visually recognized easily.

30 In addition, it is possible to reduce an area for displaying the digital signature formed by an unintelligible string having a length of 512 to 1024 bits.

Furthermore, by a combination of the MD
35 file (digest information) and authentication (password), it is possible to protect the document from being tampered with and to authenticate the

In the embodiment, the steps S13 and S14 in FIG.5 correspond to the signature generating part in claim 1 and the steps S15 and S16 in FIG.5

Also, the step S43 in FIG.7 corresponds to the signature extracting part in claim 3 and the step S44 in FIG.7 corresponds to the digest obtaining part in claim 3.

15 The present application is based on
Japanese Priority Application No. 11-332984 filed on
November 24, 1999, the entire contents of which are
hereby incorporated by reference.

WHAT IS CLAIMED IS:

5

1. An apparatus for authenticating a digital signature, comprising:

10 a signature generating part encrypting a digital document by using a private key defined by a signer and digest information for checking whether the digital document has been tampered with, and generating a digital signature;

15 a signature synthesizing part creating image information by synthesizing the digital signature and a predetermined mark; and

an image embedding part embedding the image information created by said signature synthesizing part into an indicated position in the digital document.

20

2. The apparatus as claimed in claim 1, wherein said signature synthesizing part comprises an image information generating part generating pixel data for the image information including the digital signature,

wherein:

30 a palette, where first color information is defined for first index information and second color information is defined for other index information, is referred to;

35 the first index information is defined for pixels used for the predetermined mark; and

each of the other index information, which corresponds to each number of a number string forming

09685859 101100

the digital signature, is defined for each of other pixels.

5

3. The apparatus as claimed in claim 2,
wherein said image information generating part
assigns each of the other indication information
10 corresponding to each number of the number string to
each pixel from a beginning of the number string
forming the digital signature while skipping the
pixels used for the predetermined mark.

15

4. An apparatus for authenticating a
digital signature, comprising:

20 a signature extracting part extracting the
digital signature from image information embedded
into a digital document;

a digest obtaining part decrypting the
digital signature by a public key opened by a signer
25 and obtaining first digest information for checking
whether the digital document has been tampered with;
and

an authenticating part determining whether
second digest information regenerated based on the
30 digital document identically corresponds to the first
digest information obtained by said digest obtaining
part and authenticating the digital signature based
on a result of the determination.

35

09080859 104100

5. The apparatus as claimed in claim 5,
wherein said signature extracting part refers to a
palette where first color information is defined for
first index information and second color information
5 is defined for other index information, and defines
partial pixel data, formed by removing the first
index information from pixel data forming the image
information, as the digital signature, so as to
generate the digital signature.

10

6. A method for authenticating a digital
signature, comprising the steps of:

(a) encrypting a digital document by using
a private key defined by a signer and digest
information for checking whether the digital document
has been tampered with, and generating a digital
signature;

(b) creating image information by
synthesizing the digital signature and a
predetermined mark; and

(c) embedding the image information
created in said step (b) into an indicated position
in the digital document.

30

7. A method for authenticating a digital
signature, comprising the steps of:

(a) extracting the digital signature from
image information embedded into a digital document;

(b) decrypting the digital signature by a
public key opened by a signer and obtaining first
digest information for checking whether the digital

09035359 101100

document has been tampered with; and

(c) determining whether second digest
information regenerated based on the digital document
identically corresponds to the first digest
5 information obtained by said step (b) and
authenticating the digital signature based on a
result of the determination.

10

8. A computer-readable recording medium
having a program recorded therein for causing a
computer to authenticate a digital signature, said
15 program comprising the codes of:

(a) encrypting a digital document by using
a private key defined by a signer and digest
information for checking whether the digital document
has been tampered with, and generating a digital
20 signature;

(b) creating image information by
synthesizing the digital signature and a
predetermined mark; and

(c) embedding the image information
25 created in said step (b) into an indicated position
in the digital document.

30

9. The computer-readable recording medium
as claimed in claim 8, wherein said code (b) includes
a code of (d) generating pixel data for the image
information including the digital signature,

35

wherein:

a palette, where first color information
is defined for first index information and second

09033333 101100

color information is defined for other index information, is referred to;

the first index information is defined for pixels used for the predetermined mark; and

5 each of the other index information, which corresponds to each number of a number string forming the digital signature, is defined for each of other pixels.

10

10. The computer-readable recording medium as claimed in claim 9, wherein said code (d)
15 assigns each of the other indication information corresponding to each number of the number string to each pixel from a beginning of the number string forming the digital signature while skipping the pixels used for the predetermined mark.

20

11. A computer-readable recording medium
25 having a program recorded therein for causing a computer to authenticate a digital signature, said program comprising the codes of:

(a) extracting the digital signature from image information embedded into a digital document;

30 (b) decrypting the digital signature by a public key opened by a signer and obtaining first digest information for checking whether the digital document has been tampered with; and

(c) determining whether second digest
35 information regenerated based on the digital document identically corresponds to the first digest information obtained by said code (b) and

0568333 101100

authenticating the digital signature based on a
result of the determination.

5

12. The computer-readable recording
medium as claimed in claim 11, wherein said signature
extracting part refers to a palette where first color
10 information is defined for first index information
and second color information is defined for other
index information, and defines partial pixel data,
formed by removing the first index information from
pixel data forming the image information, as the
15 digital signature, so as to generate the digital
signature.

09083359 104100

ABSTRACT OF THE DISCLOSURE

In an apparatus for authenticating a digital signature, a signature generating part encrypts a digital document by using a private key
5 defined by a signer and digest information for checking whether the digital document has been tampered with, and generates a digital signature. A signature synthesizing part creates image information by synthesizing the digital signature and a
10 predetermined mark. And an image embedding part embeds the image information created by said signature synthesizing part into an indicated position in the digital document.

09635859 101100

FIG. 2

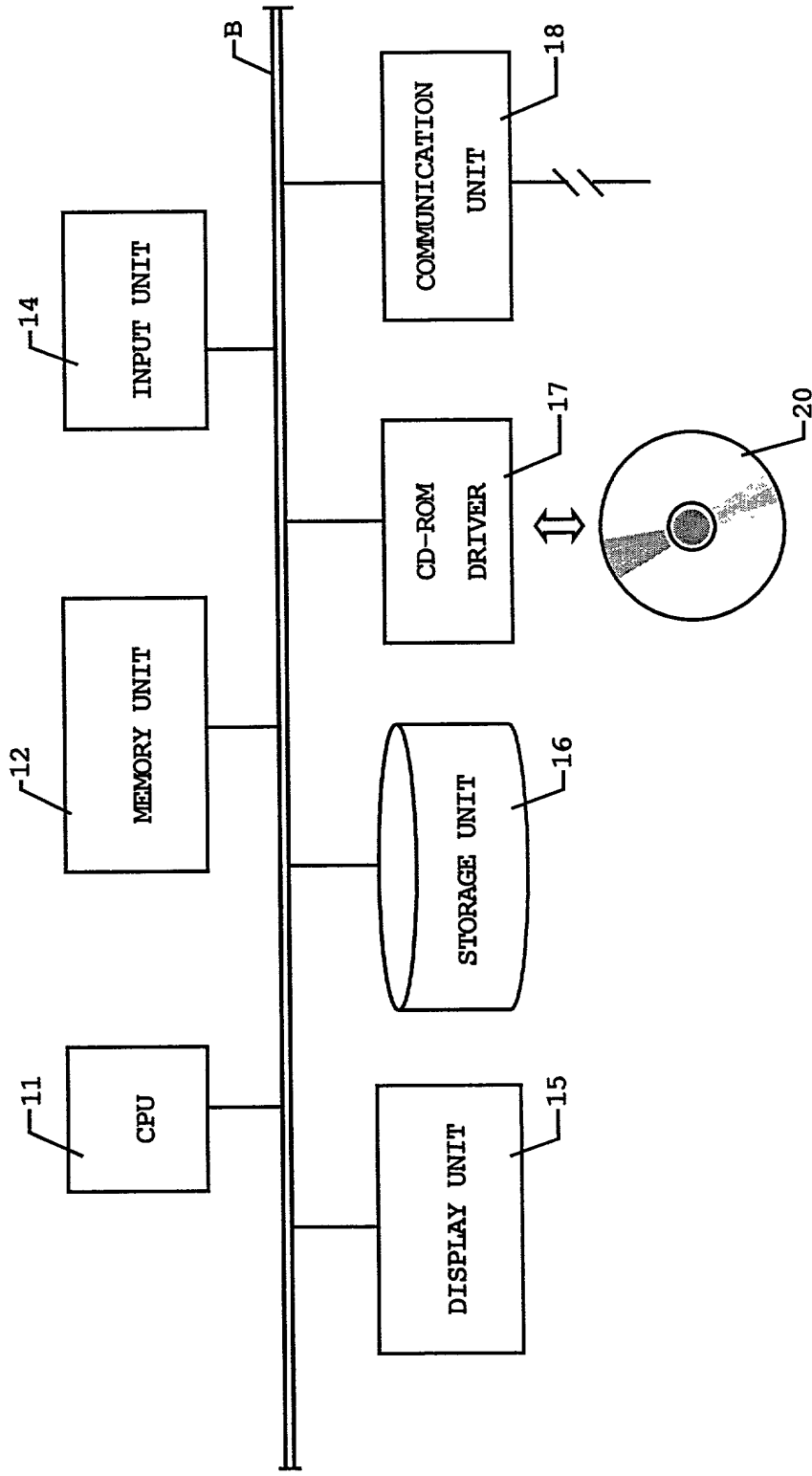
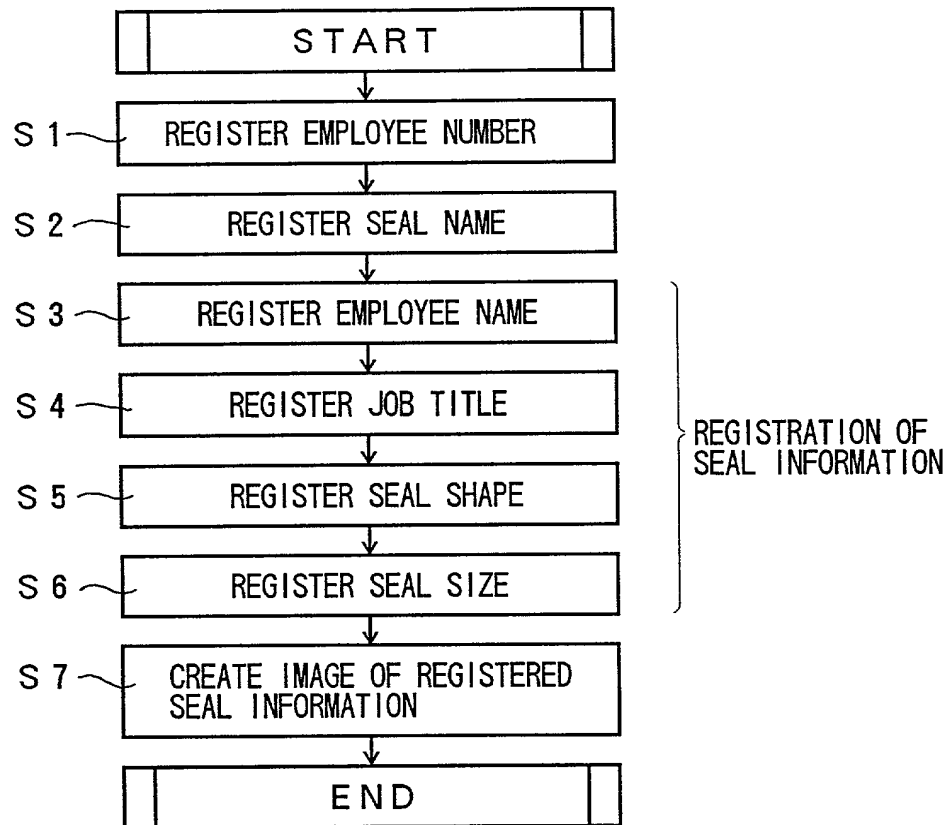


FIG. 3



Introduction

Introduction

Introduction

Introduction

FIG. 5

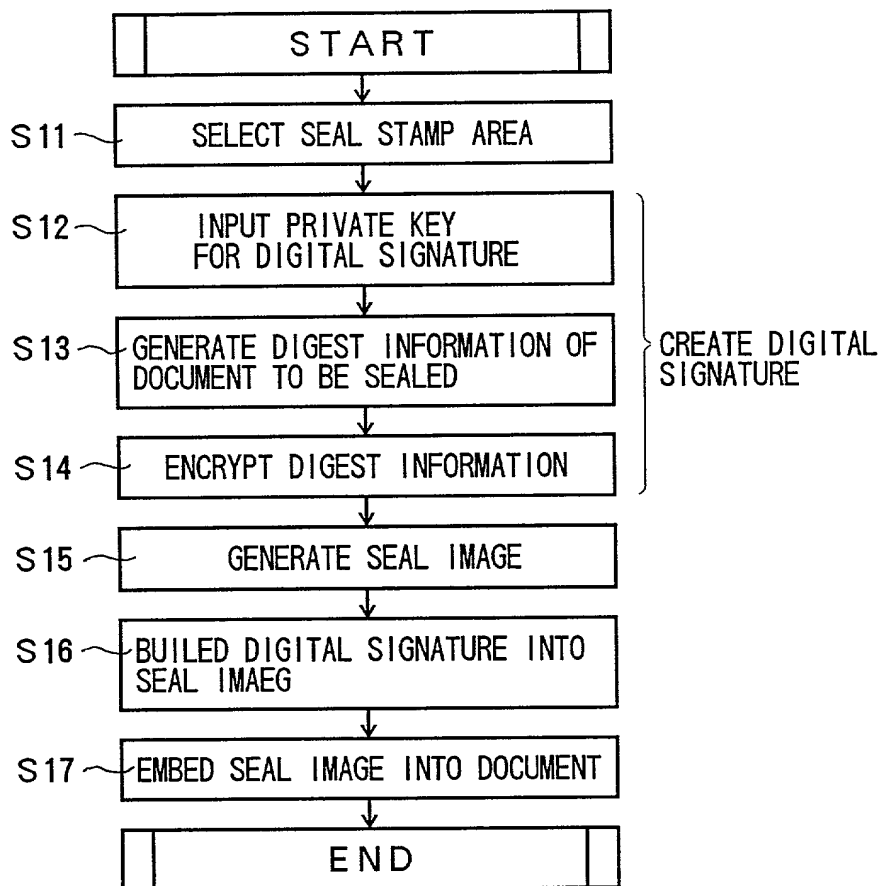


FIG. 6A

STAMP

EXECUTION OF SEAL STAMP

STAMP YOUR SEAL IN THE SELECTED AREA

EMPLOYEE NUMBER: 1 2 3 4 5 6 7 8 9 0

SEAL NAME :

PRIVATE KEY : *****

☐ CONFIRM WHEN YOUR DOCUMENT IS DISPLAYED

STAMP CANCEL

FIG. 6B

STAMP

DEVELOPMENT
SECTION MANAGER

03. 03. 98

FUJI

CONFIRMATION OF STAMPED SEAL

STAMPED YOUR SEAL IN THE SELECTED AREA

OK CANCEL

FIG. 7

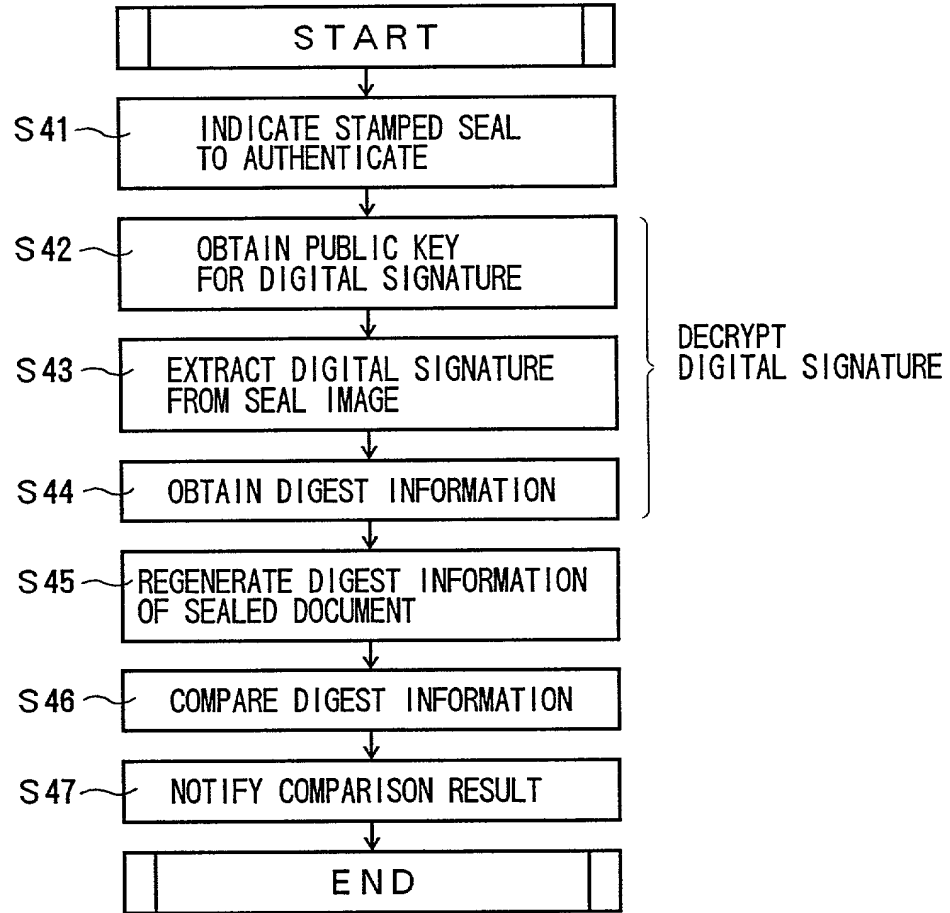


FIG. 8A

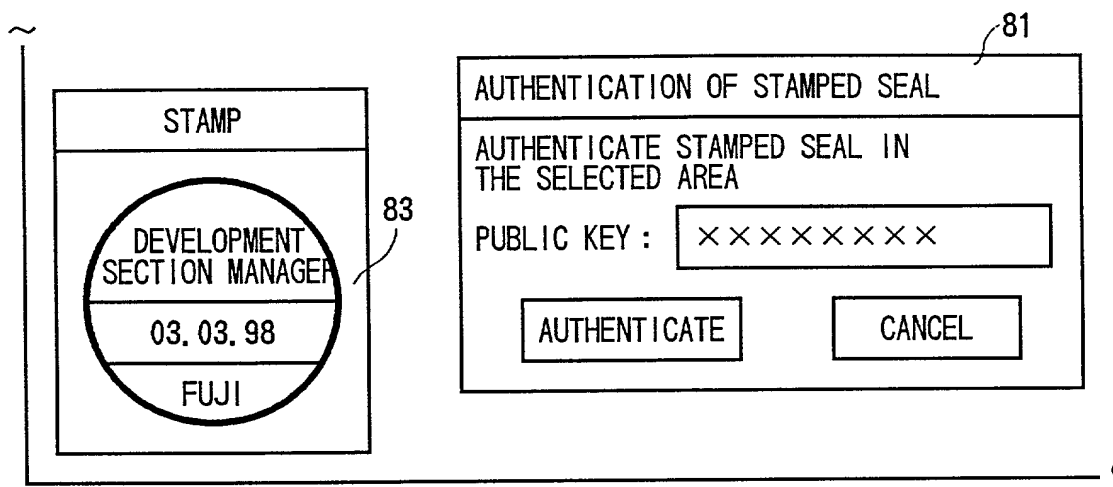


FIG. 8B

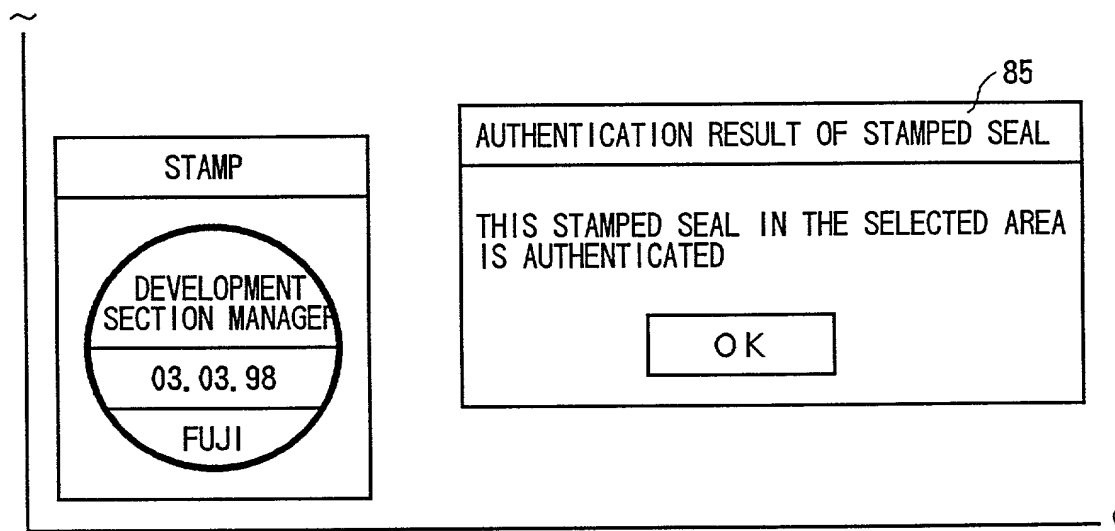
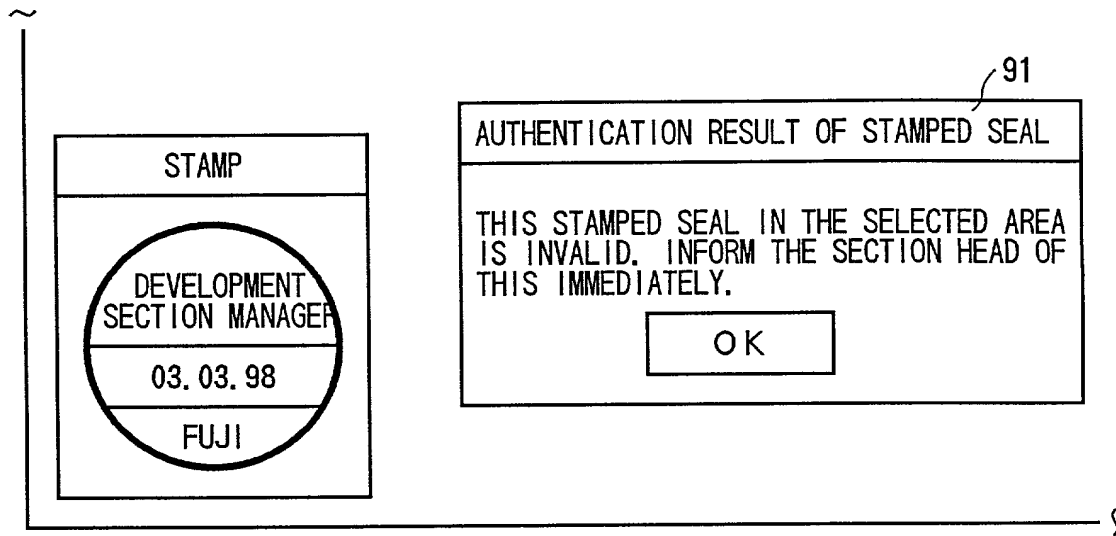
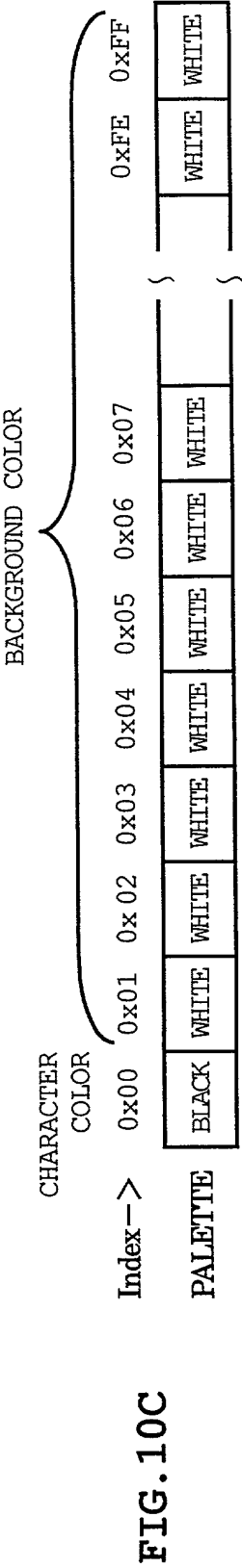
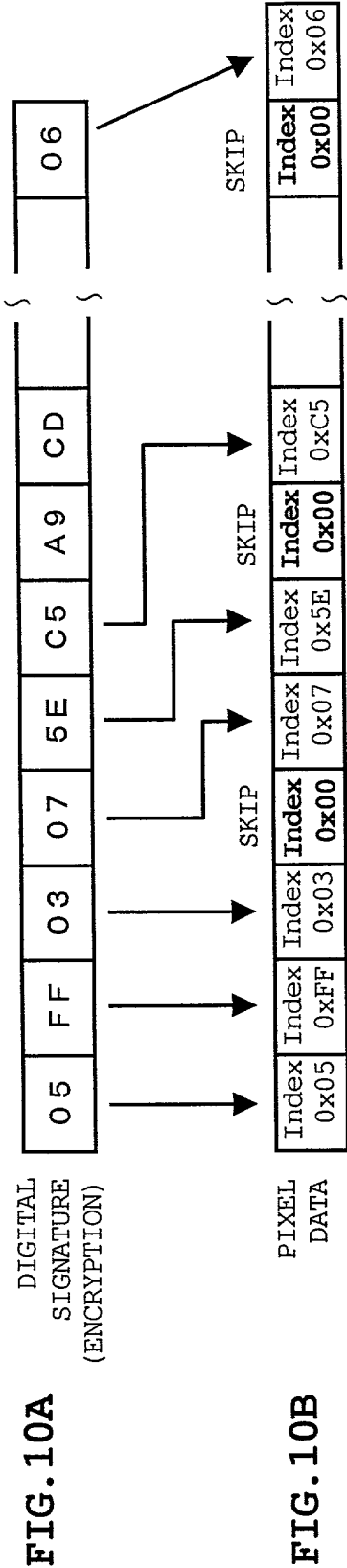


FIG. 9





Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Declaration and Power of Attorney For Patent Application

特許出願宣言書及び委任状

Japanese Language Declaration

日本語宣言書

下記の氏名の発明者として、私は以下の通り宣言します。

As a below named inventor, I hereby declare that:

私の住所、私書箱、国籍は下記の私の氏名の後に記載された通りです。

My residence, post office address and citizenship are as stated next to my name.

下記の名称の発明に関して請求範囲に記載され、特許出願している発明内容について、私が最初かつ唯一の発明者（下記の氏名が一つの場合）もしくは最初かつ共同発明者であると（下記の名称が複数の場合）信じています。

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

APPARATUS AND METHOD FOR AUTHENTICATING
DIGITAL SIGNATURES AND COMPUTER-READABLE
RECORDING MEDIUM THEREOF

上記発明の明細書（下記の欄でx印がついていない場合は、本書に添付）は、

the specification of which is attached hereto unless the following box is checked:

☐ 月 日に提出され、米国出願番号または特許協定条約
国際出願番号を _____ とし、
(該当する場合) _____ に訂正されました。

☐ was filed on _____
as United States Application Number or
PCT International Application Number
_____ and was amended on
_____ (if applicable).

私は、特許請求範囲を含む上記訂正後の明細書を検討し、
内容を理解していることをここに表明します。

I hereby state that I have reviewed and understand the contents of
the above identified specification, including the claims, as
amended by any amendment referred to above.

私は、連邦規則法典第37編第1条56項に定義されると
おり、特許資格の有無について重要な情報を開示する義務が
あることを認めます。

I acknowledge the duty to disclose information which is material to
patentability as defined in Title 37, Code of Federal Regulations,
Section 1.56.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Japanese Language Declaration (日本語宣言書)

私は、米国法典第35編119条(a)-(d)項又は365条(b)項に基づき下記の、米国以外の国の少なくとも一カ国を指定している特許協力条約365(a)項に基づく国際出願、又は外国での特許出願もしくは発明者証の出願についての外国優先権をここに主張するとともに、優先権を主張している、本出願の前に出願された特許または発明者証の外国出願を以下に、枠内をマークすることで、示しています。

Prior Foreign Application(s)

Pat. Appln. No. 11-332984

Japan

I hereby claim foreign priority under Title 35, United States Code, Section 119 (a)-(d) or 365(b) of any foreign application(s) for patent or inventor's certificate, or 365(a) of any PCT International application which designated at least one country other than the United States, listed below and have also identified below, by checking the box, any foreign application for patent or inventor's certificate, or PCT International application having a filing date before that of the application on which priority is claimed.

Priority Not Claimed

優先権主張なし

(Number)
(番号)

(Country)
(国名)

24/November/1999
(Day/Month/Year Filed)
(出願年月日)

☐

(Number)
(番号)

(Country)
(国名)

(Day/Month/Year Filed)
(出願年月日)

☐

私は、第35編米国法典119条(e)項に基づいて下記の米国特許出願規定に記載された権利をここに主張いたします。

I hereby claim the benefit under Title 35, United States Code, Section 119(e) of any United States provisional application(s) listed below.

(Application No.)
(出願番号)

(Filing Date)
(出願日)

(Application No.)
(出願番号)

(Filing Date)
(出願日)

私は、下記の米国法典第35編120条に基づいて下記の米国特許出願に記載された権利、又は米国を指定している特許協力条約365条(c)に基づき権利をここに主張します。また、本出願の各請求範囲の内容が米国法典第35編112条第1項又は特許協力条約で規定された方法で先行する米国特許出願に開示されていない限り、その先行米国出願を提出日より本出願書の日本国内または特許協力条約国際提出日までの期間中に入手された、連邦規則法典第37編1条56項で定義された特許資格の有無に関する重要な情報について開示義務があることを認識しています。

I hereby claim the benefit under Title 35, United States Code, Section 120 of any United States application(s), or 365(c) of any PCT International application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of Title 35, United States Code Section 112, I acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56 which became available between the filing date of the prior application and the national or PCT International filing date of application.

(Application No.)
(出願番号)

(Filing Date)
(出願日)

(Status: Patented, Pending, Abandoned)
(現況: 特許許可済、係属中、放棄済)

(Application No.)
(出願番号)

(Filing Date)
(出願日)

(Status: Patented, Pending, Abandoned)
(現況: 特許許可済、係属中、放棄済)

私は、私自身の知識に基づいて本宣言書中で私が行なう表明が真実であり、かつ私の入手した情報と私の信じていることに基づき表明が全て真実であると信じていること、さらに故意になされた虚偽の表明及びそれと同等の行為は米国法典第18編第1001条に基づき、罰金または拘禁、もしくはその両方により処罰されること、そしてそのような故意による虚偽の表明を行えば、出願した、又は既に許可された特許の有効性が失われることを認識し、よってここに上記のごとく宣誓を致します。

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Japanese Language Declaration

(日本語宣言書)

委任状： 私は下記の発明者として、本出願に関する一切の
手続きを米特許商標局に対して遂行する弁理士または代理人
として、下記の者を指名いたします。（弁理士、または代理
人氏名及び登録番号を明記のこと）

POWER OF ATTORNEY: As a named inventor, I hereby appoint
the following attorney(s) and/or agent(s) to prosecute this
application and transact all business in the Patent and Trademark
Office connected therewith (list name and registration number)

James D. Halsey, Jr., 22,729; Harry John Staas, 22,010; David M. Pitcher, 25,908; John C. Garvey, 28,607; J. Randall Beckers, 30,358;
William F. Herbert, 31,024; Richard A. Gollhofer, 31,106; Mark J. Henry, 36,162; Gene M. Garner II, 34,172; Michael D. Stein, 37,240; Paul
I. Kravetz, 35,230; Gerald P. Joyce, III, 37,648; Todd E. Mariette, 35,269; Harlan B. Williams, Jr., 34,756; George N. Stevens, 36,938;
Michael C. Soldner, P-41,455 and William M. Schertler, 35,348 (agent)

送付先

Send Correspondence to:

STAAS & HALSEY
700 Eleventh Street, N.W.
Suite 500
Washington, D.C. 20001

直接電話連絡先：（名前及び電話番号）

Direct Telephone Calls to: (name and telephone number)

STAAS & HALSEY
(202) 434-1500

唯一または第一発明者名	Full name of sole or first inventor		
	Syuichi Satake		
発明者の署名	日付	Inventor's signature	Date
		Syuichi Satake	September 25, 2000
住所	Residence		
	Nei, Japan		
国籍	Citizenship		
	Japan		
私書箱	Post Office Address		
	c/o TOYAMA FUJITSU LIMITED, 2-1, Yasuuchi 2-chome, Yatsuo Machi, Nei-Gun, Toyama, 939-2392 Japan		
第二共同発明者	Full name of second joint inventor, if any		
第二共同発明者	日付	Second inventor's signature	Date
住所	Residence		
国籍	Citizenship		
私書箱	Post Office Address		

（第三以降の共同発明者についても同様に記載し、署名をす
ること）

(Supply similar information and signature for third and subsequent
joint inventors.)